



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/854,493	05/15/2001	Daniel Joseph Wolff	550-231	7924
23117	7590	07/29/2005	EXAMINER	
NIXON & VANDERHYE, PC 901 NORTH GLEBE ROAD, 11TH FLOOR ARLINGTON, VA 22203			HO, THOMAS M	
			ART UNIT	PAPER NUMBER
			2134	
DATE MAILED: 07/29/2005				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/854,493

Applicant(s)

WOLFF ET AL.

Examiner

Thomas M. Ho

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on 22 April 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-27 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-27 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 22 April 2005 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 6/13/02.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. **The amendment of 4/22/05 has been received and entered.**
2. Claims 1-27 are pending

Response to Arguments

3. Applicant's arguments with respect to claims 1-27 have been considered but are moot in view of the new ground(s) of rejection as necessitated by amendment.

The Examiner however, disagrees with Applicant's assertion that "Having the archived copy allows for the direct comparison which is not disclosed in Dyson. In fact, Dyson does not even disclose an archived copy of the file." (page 11, paragraph 3, arguments)

The Examiner contends that Dyson explicitly discloses having an archived copy.

Dyson (Column 3, line 55 – Column 4, line 17) disclose that a first copy of a file is sent towards another storage location. At a later time, when a second unverified file needs to be verified, the comparison of the part of the file which is the identifier verifies the integrity of the second file such that a match would indicate that the files are identical. (Column 4, lines 15-17)

Furthermore, Dyson himself states in the abstract that his invention is:

"A method and apparatus for verifying a file stored separately from a computer to be identical with a previous version of the file..."

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-27 are rejected under 35 U.S.C. 102(b) as being anticipated by Dyson, US patent 5,050,212.

In reference to claim 1:

Dyson (Column 4, lines 10-25) discloses a computer program product comprising a computer program operable to control a computer to detect a malicious alteration to a stored computer file, said computer program comprising:

- File comparing logic operable to compare said stored computer file with an archive copy of said computer file stored when said stored computer file was created(Figure 2, step 4) & (Column 5, lines 5-8) & (Column 4, lines 10-25)
- Comparison response logic operable if said file comparing logic detects that said stored computer file and said archive computer file do not match to trigger further countermeasures against a potential malicious alteration. (Column 4, lines 10-25)

Art Unit: 2134

Dyson fails to disclose an embodiment where the entire contents of one file are compared with the contents of another file. Dyson rather, discloses a comparison being performed based on the hash IDs.

The Examiner takes official notice that comparing the entire contents of one file to another file was well known in the art at the time of invention.

For Example.

Jamsa "Comparing two files with COMP" (pgs. 392-401, 406-407) discloses a method of comparing two files exactly by comparing the contents byte for byte.

Jamsa "Comparing files with FC" (pgs. 392-401, 406-407) yet again discloses a method of comparing the contents of two files exactly byte for byte provided that the switch /B is used with the command.

Both of these commands are commands as part of the publicly sold and used DOS operating system at least as of 1991. Furthermore, DOS was an extremely widely used operating system in the field of computer science with over fifty million users as of the publication date of the book.

Jamsa "Introduction", page xxiii, "there are over 50 million DOS users..."

The well known advantage of comparing two files in their entirety is providing a more accurate comparison. Applicant appears to recognize this advantage as well. Page 11 of the arguments

Art Unit: 2134

states “Comparing the entire file contents is thus more accurate and reliable than comparing file hash values.”

It would have been obvious to one of ordinary skill in the art at the time of invention to directly compare the entire contents of the stored computer files to determine file alteration in order to make a more accurate judgment between the comparisons.

In reference to claim 2:

Dyson fails to disclose a computer program product as claimed in claim 1, wherein said further countermeasures include scanning said stored computer file using a library of computer virus definition data to identify a computer virus infection of said stored computer file.

Dyson however, does teach that viruses are often the element that causes malicious changes to the files. (Column 1, lines 17-21)

The Examiner takes official notice that virus scanning modules were well known in the art at the time of invention. Such Examples included, Norton Antivirus TM and McAfee Antivirus Software TM. Programs such as Norton Antivirus use a library of computer virus definition data in order to identify which virus, if any, your file is infected with. Virus definition files must be updated every so often, as new viruses are always being developed.

Art Unit: 2134

It would have been obvious to one of ordinary skill in the art at the time of invention to apply antivirus software in order to clear files of viruses, given the knowledge that viruses are often the cause of malicious changes to files.

In reference to claim 3:

Dyson (Figure 2, steps 3 and 4) & (Column 3, lines 57-62) discloses a computer program product as claimed in claim 1, wherein said archive copy of said computer file is stored in one of:

- An unencrypted form;
- An encrypted form;
- An encrypted media
- An encrypted volume
- A PGP disk.

Where the archive copy is stored in both an unencrypted form, with an encrypted portion.

In reference to claim 4:

Dyson (Column 2, lines 40-45) discloses a computer program product as claimed in claim 1, wherein said archive copy of said computer file is stored in one of:

- A different physical storage device to said stored computer file
- A different part of a common physical storage device shared with stored computer file.

(Column 4, line 67 – Column 5, line 5)

Where the computer program product is stored in a different physical storage location.

In reference to claim 5:

Dyson (Column 4, lines 10-25) & (Column 2, line 57 – Column 3, line 10) discloses a computer program product as claimed in claim 1, wherein a subset of file types stored by said computer are subject comparison by said file comparing logic and to creation of an archive copy for use with said file comparing logic, where Dyson discloses that the preferred embodiment examines boot file executables, and that the integrity check or file comparing logic is used on these subset of files.

In reference to claim 6:

Dyson (Column 2, line 57 – Column 3, line 10) discloses a computer program product as claimed in claim 5, wherein said subset of file types include one or more of:

- Executable file types (Column 2, line 62)
- Dynamic link library file types. (Column 3, lines 4-6)

In reference to claim 7:

Dyson (Figure 2, steps 3 and 4) discloses a computer program product as claimed in claim 1, comprising archive file copy logic operable upon creation of said stored computer file to also created said archive copy of said computer file, where the header and the logic hash to be compared is created and stored with the local computer file and the archived one. (Column 4, lines 5-10)

Claim 8 is substantially similar to claim 5 and is rejected for the same reasons.

Claim 9 is substantially similar to claim 6 and is rejected for the same reasons.

Claims 10, 12-18 are a branch of claims substantially similar to claims 1, 3-9, respectively, and are rejected for the same reasons.

Claims 19, 21-27 are a branch of claims substantially similar to claims 1, 3-9, respectively, and are rejected for the same reasons.

Conclusion

6. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of the final action and the advisory action is not mailed under after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension pursuant to 37 CFR 1.136(A) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

7. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (571)272-3838.

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist	Telephone: 571-272-2100	Fax: 703-872-9306
Customer Service Representative	Telephone: 571-272-2100	Fax: 703-872-9306

TMH

July 14, 2005

David Y. Jung
Primary Examiner

7/21/05
D. Jung